(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
8. Februar 2001 (08.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/09847 A1

(51) Internationale Patentklassifikation[7]: G07C 9/00

(21) Internationales Aktenzeichen: PCT/EP00/07124

(22) Internationales Anmeldedatum:
25. Juli 2000 (25.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 36 094.4 30. Juli 1999 (30.07.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, D-81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **MÖDL, Albert** [DE/DE]; Walter-Kollo-Strasse 21, D-86368 Gersthofen (DE). **STEPHAN, Elmar** [DE/DE]; Danklstrasse 13, D-81371 München (DE). **MÜLLER, Robert** [DE/DE]; Hansjakobstrasse 80, D-81673 München (DE).

(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, D-80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: METHOD, DEVICE AND SYSTEM FOR BIOMETRIC AUTHENTICATION

(54) Bezeichnung: VERFAHREN, VORRICHTUNG UND SYSTEM ZUR BIOMETRISCHEN AUTHENTISIERUNG

(57) Abstract: The invention relates to a method, device and system for biometric authentication which safeguards against replay attacks. In biometric authentication, a biometric characteristic presented by a person, for example, a fingerprint, or a personal signature is presented and compared with previously saved reference data. The invention aims to prevent the biometric data from being intercepted and used again for an unauthorised authentication. To this end, an authentication containing data for the presented biometric characteristic which corresponds 100 % or even 99 % with the saved reference data is rejected, as it is recognised that biometric characteristics cannot usually be recorded so that they can be 100 % reproduced and such a case can thus be assumed to be a replay attack. In one embodiment, the presented biometric characteristics are collected, saved and then taken into consideration in subsequent inspections of authentication procedures for replay attacks.

(57) Zusammenfassung: Es wird ein Verfahren, eine Vorrichtung und ein System zur biometrischen Authentisierung vorgeschlagen, das gegen Replay-Angriffe gesichert ist. Bei der biometrischen Authentisierung wird ein von einer Person präsentiertes biometrisches Merkmal, beispielsweise ein Fingerabdruck oder die persönliche Unterschrift, präsentiert und mit zuvor abgespeicherten Referenzdaten verglichen. Um zu verhindern, daß die biometrischen Daten abgefangen und nochmals für eine unberechtigte Authentisierung verwendet werden, sieht die Erfindung vor, daß eine Authentisierung bei 100 %iger Übereinstimmung oder auch nur bei 99 %iger Übereinstimmung der Daten des präsentierten biometrischen Merkmals mit den gespeicherten Referenzdaten verweigert wird. Denn biometrische Merkmale haben in aller Regel die Eigenschaft, daß sie nicht 100 %ig reproduzierbar erfaßt werden können, so daß in solchen Fällen von einem Replay-Angriff ausgegangen werden kann. In einer Ausgestaltung der Erfindung werden die präsentierten biometrischen Merkmale gesammelt und gespeichert und in nachfolgenden Authentisierungsverfahren bei der Prüfung auf Replay-Angriffe berücksichtigt.

WO 01/09847 A1

Diese Aufgabe wird erfindungsgemäß durch die Merkmale der nebengeordneten Ansprüche gelöst. In Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung angegeben.

Die Erfindung macht sich zunutze, daß den biometrischen Merkmalen in aller Regel gemeinsam ist, daß sie im Gegensatz zur PIN nicht 100%ig reproduzierbar sind, weswegen eine Autorisierung auch bereits schon dann erfolgt, wenn die Übereinstimmung des von der Person präsentierten biometrischen Merkmals mit den gespeicherten Referenzdaten einen vorgegebenen Schwellwert überschreitet. Erfindungsgemäß ist nun vorgesehen, daß die Übereinstimmung nicht über einem (zweiten) vorgegebenen Schwellwert liegen darf, insbesondere nicht 100% und vorzugsweise nicht mehr als 99% betragen darf. Im Falle einer derart großen Übereinstimmung kann nämlich von einem Replay-Angriff ausgegangen werden, und gemäß der Erfindung wird die Authentisierung demzufolge verweigert. Dazu ist eine Vergleichschaltung vorgesehen, die eine Meldung erzeugt und beispielsweise eine Fehlermeldung ausgegeben, wenn ein Vergleich der Referenzdaten mit den neu erfaßten biometrischen Daten einer Person eine über diesem (zweiten) Schwellwert liegende Übereinstimmung ergibt. Wird die Fehlermeldung ausgegeben, kann es auch vorgesehen sein, den weiteren Betrieb automatisch zu sperren.

Als Beispiel sei der Vergleich zweier Unterschriften von ein und derselben Person genannt. Diese Unterschriften mögen visuell betrachtet deckungsgleich sein, sie können aber bei einer Auflösung von beispielsweise 500 dpi niemals pixelweise zur Deckung gebracht werden. Bei Berücksichtigung der dynamischen Anteile in der Unterschrift gibt es noch weitere Freiheitsgrade und natürliche Abweichungen.

Verfahren, Vorrichtung und System zur biometrischen Authentisierung

Die Erfindung betrifft ein Verfahren, sowie eine Vorrichtung und ein System zur biometrischen Authentisierung, insbesondere zur Sicherung der biometrischen Authentisierung gegen Replay-Angriffe.

Ein Authentisierungsverfahren findet Anwendung, wenn eine Person Zugang zu gesicherten Einrichtungen begehrt. Beispielsweise erfolgt eine Authentisierung regelmäßig mittels eines PIN-Vergleichs, wenn ein Kartenbenutzer eine Chipkarte - beispielsweise eine Kreditkarte - in einen Bankautomaten (Terminal) einführt oder wenn eine Person zu zugangsgesicherten Räumlichkeiten Eintritt begehrt. Dazu wird eine gespeicherte PIN mit der vom Kartenbenutzer bzw. von der Eintritt begehrenden Person angegebenen PIN auf Identität überprüft.

Im Falle eines biometrischen Authentisierungsverfahrens wird anstatt einer PIN ein biometrisches Merkmal der Person als Identifikationsmerkmal benutzt. Das biometrische Merkmal kann beispielsweise ein Fingerabdruck sein, soll im Sinne der vorliegenden Erfindung aber auch eine persönliche Unterschrift umfassen. Nachteilhaft bei solchen Authentisierungsverfahren ist, daß ein Angriff auf die Authentisierung möglich ist, wenn die biometrischen Daten, die als Referenzdaten abgespeichert wurden oder die zu einer Authentisierung geführt haben, von nicht autorisierten Dritten abgefangen werden, um sie später erneut für eine unberechtigte Authentisierung zu verwenden. Diese Art des Angriffs wird als Replay-Angriff bezeichnet.

Aufgabe der vorliegenden Erfindung ist es daher, biometrische Authentisierungsverfahren gegen Replay-Angriffe zu sichern.

Der für die Erfindung relevante (zweite) Schwellwert von 99% oder 100% wird entweder in einem Terminal oder auf einem separaten Datenträger, insbesondere einer Chipkarte, zusammen mit den Referenzdaten gespeichert.

In einer bevorzugten Ausgestaltung der Erfindung ist vorgesehen, daß die erfaßten biometrischen Daten, die zu einer Authentisierung geführt haben und gegebenenfalls auch diejenigen erfaßten biometrischen Daten, die nicht zur Authentisierung führten, weil sie unterhalb des ersten Schwellwerts lagen, gesammelt und als Datensätze gespeichert werden. Vorzugsweise werden diese Datensätze in einem Stapelspeicher oder Schieberegister gespeichert. Bei jedem Authentisierungsvorgang wird dann geprüft, ob die biometrischen Daten des präsentierten biometrischen Merkmals mit einem der gespeicherten Datensätze identisch sind oder gegebenenfalls zu mehr als 99% übereinstimmen. Dann kann von einem Replay-Angriff ausgegangen werden, und die Authentisierung wird von dem Authentisierungssystem verweigert.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung werden anstatt der oder zusätzlich zu den zuletzt von der Chipkarte empfangenen biometrischen Vergleichsdatensätze Hashwerte derselben abgespeichert. Hierzu wird eine Hash-Funktion auf den Vergleichsdatensatz angewandt, welche einen relativ kurzen Hashwert erzeugt. Hash-Funktionen sind an sich bekannt, wobei eine Hash-Funktion eine eindeutige, komprimierende Abbildung auf ein Wort fester Länge ist. Die Hash-Funktion wird in mehreren Runden auf einer blockweisen Partition der Ausgangsdaten abgearbeitet. Das Ergebnis hängt dabei von der gesamten Eingabe ab. Eine Berechnung der Ausgangsdaten aus dem Hashwert ist nicht möglich. Es ist komplexitätstheoretisch

schwierig, die Eingabedaten gezielt so zu ändern, daß der Hashwert derselbe bleibt.

Werden ein weiteres Mal Merkmale präsentiert und daraus berechnete Biometriedaten in die Karte eingebracht, so wird der Hashwert erneut berechnet. Die Wahrscheinlichkeit, daß zwei biometrische Datensätze denselben Hashwert erzeugen, ist gering, so daß bei Übereinstimmung von einem Replay-Angriff ausgegangen werden muß. Durch die Verwendung der Hashwerte sind bei der Umsetzung der Erfindung erhebliche Einspa-rungen an Speicherplatz und Verarbeitungszeit möglich. Die Speicherung mehrerer Hashwerte fester Länge in einer Art Schieberegister ist hier einfach, da ein Hashwert üblicherweise nur wenige Bytes Speicherplatz benötigt.

Patentansprüche

1. Verfahren zur Sicherung einer biometrischen Authentisierung gegen Replay-Angriffe, wobei ein Vergleich zwischen als Referenzdaten gespeicherten biometrischen Daten einer Person und erneut erfaßten biometrischen Daten der Person auf Übereinstimmung durchgeführt wird und anhand des Vergleichs eine Authentisierung erfolgt, **dadurch gekennzeichnet,** daß die Authentisierung verweigert wird, wenn durch den Vergleich eine Übereinstimmung der erneut erfaßten biometrischen Daten mit den gespeicherten Referenzdaten festgestellt wird, die gleich oder größer einem vorgegebenen Schwellwert ist.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß der Schwellwert bei 100%iger Übereinstimmung festgelegt wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet,** daß die bei verschiedenen Authentisierungsvorgängen erfaßten biometrischen Daten als Datensätze gesammelt und gespeichert werden und die Authentisierung verweigert wird, wenn die erneut erfaßten biometrischen Daten eines aktuellen Authentisierungsvorgangs im Vergleich zu einem der gespeicherten Datensätze eine über dem vorgegebenen Schwellwert liegende Übereinstimmung aufweisen.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** daß der Schwellwert bei mindestens 99%iger Datenübereinstimmung festgelegt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß die Referenzdaten und gegebenenfalls die Datensätze auf einem Datenträger, insbesondere einer Chipkarte, gespeichert werden.

6. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß die Referenzdaten und gegebenenfalls die Datensätze in einer Authentisierungsvorrichtung, insbesondere einem Chipkartenterminal, gespeichert werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet,** daß aus den erneut erfaßten biometrischen Daten ein Hashwert gebildet wird und daß die gespeicherten Referenzdaten ein Hashwert sind.

8. Vorrichtung zur biometrischen Authentisierung, umfassend einen ersten Speicherbereich mit biometrischen Daten als Referenzdaten und eine Vergleichsschaltung, die eine Meldung erzeugt, wenn ein Vergleich der Referenzdaten mit neu erfaßten biometrischen Daten einer Person eine Übereinstimmung ergibt, die gleich oder größer einem gegebenen Schwellwert ist.

9. Vorrichtung nach Anspruch 8, **dadurch gekennzeichnet,** daß die Vorrichtung ein Datenträger, insbesondere eine Chipkarte, ist.

10. Vorrichtung nach Anspruch 8 oder 9, **dadurch gekennzeichnet,** daß der Schwellwert auf 100% eingestellt ist.

11. Vorrichtung nach einem der Ansprüche 8 bis 10, **gekennzeichnet durch** weitere Speicherbereiche, in denen mehrere Datensätze von erneut erfaßten biometrischen Daten gespeichert sind.

12. Vorrichtung nach Anspruch 11, **dadurch gekennzeichnet,** daß die weiteren Speicherbereiche einen Stapelspeicher bilden.

13. Vorrichtung nach Anspruch 11, **dadurch gekennzeichnet,** daß die weiteren Speicherbereiche ein Schieberegister bilden.

14. Vorrichtung nach einem der Ansprüche 8 bis 13, **dadurch gekennzeichnet,** daß der Schwellwert auf einen Wert ≥ 99% eingestellt ist.

15. Vorrichtung nach einem der Ansprüche 8 bis 14, **dadurch gekennzeichnet,** daß sich die Vorrichtung bei Vorliegen der Meldung automatisch sperrt.

16. Vorrichtung nach einem der Ansprüche 8 bis 15, **dadurch gekennzeichnet,** daß die Vorrichtung bei Vorliegen der Meldung eine Fehlermeldung ausgibt.

17. Vorrichtung nach einem der Ansprüche 8 bis 16, **dadurch gekennzeichnet,** daß im ersten Speicherbereich als Referenzdaten ein aus biometrischen Daten abgeleiteter Hashwert gespeichert ist und daß die Vergleichsschaltung aus den neu erfaßten biometrischen Daten einen Hashwert für den Vergleich mit den gespeicherten Referenzdaten bildet.

18. System zur biometrischen Authentisierung, umfassend eine Vorrichtung nach einem der Ansprüche 8 bis 17 und einer Einrichtung zum Erfassen biometrischer Daten einer Person.

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 870 723 A (HOFFMAN NED ET AL) 9 February 1999 (1999-02-09)	1-3,8, 10,11, 15,16,18
Y	column 2, line 11 -column 4, line 49 column 36, line 7 - line 39	5,6,9
X	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19 March 1998 (1998-03-19) page 3, line 22 -page 5, line 25 page 10, line 11 -page 11, line 30	1,2, 7-10,15, 17,18
Y	US 5 280 527 A (FAST NORMAN ET AL) 18 January 1994 (1994-01-18) abstract column 5, line 34 - line 54	5,6,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 November 2000	09/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Teutloff, H

Angaben zu Veröffentlichunge zur selben Patentfamilie gehören

Interna[illegible]les Aktenzeichen
/EP 00/07124

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5870723 A	09-02-1999	US 5613012 A	18-03-1997
		US 5615277 A	25-03-1997
		AU 4329597 A	19-03-1998
		WO 9809227 A	05-03-1998
		US 6012039 A	04-01-2000
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		EP 0912959 A	06-05-1999
		JP 11511882 T	12-10-1999
		WO 9636934 A	21-11-1996
		US 5838812 A	17-11-1998
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
		EP 0931430 A	28-07-1999
US 5280527 A	18-01-1994	CA 2105404 A	03-03-1995

INTERNATIONALER RECHERCHENBERICHT

Interr ...les Aktenzeichen
PCT/E ...)/07124

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 870 723 A (HOFFMAN NED ET AL) 9. Februar 1999 (1999-02-09)	1-3,8, 10,11, 15,16,18
Y	Spalte 2, Zeile 11 -Spalte 4, Zeile 49 Spalte 36, Zeile 7 - Zeile 39	5,6,9
X	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19. März 1998 (1998-03-19) Seite 3, Zeile 22 -Seite 5, Zeile 25 Seite 10, Zeile 11 -Seite 11, Zeile 30	1,2, 7-10,15, 17,18
Y	US 5 280 527 A (FAST NORMAN ET AL) 18. Januar 1994 (1994-01-18) Zusammenfassung Spalte 5, Zeile 34 - Zeile 54	5,6,9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. November 2000	09/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Teutloff, H

2

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5870723 A	09-02-1999	US 5613012 A	18-03-1997
		US 5615277 A	25-03-1997
		AU 4329597 A	19-03-1998
		WO 9809227 A	05-03-1998
		US 6012039 A	04-01-2000
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		EP 0912959 A	06-05-1999
		JP 11511882 T	12-10-1999
		WO 9636934 A	21-11-1996
		US 5838812 A	17-11-1998
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
		EP 0931430 A	28-07-1999
US 5280527 A	18-01-1994	CA 2105404 A	03-03-1995

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
K 51 513/7ch		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 00/ 07124	25/07/2000	30/07/1999
Anmelder		
GIESECKE & DEVRIENT GMBH		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. ---

   [ ] wie vom Anmelder vorgeschlagen

   [X] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/07124

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 870 723 A (HOFFMAN NED ET AL) 9. Februar 1999 (1999-02-09)	1-3,8, 10,11, 15,16,18
Y	Spalte 2, Zeile 11 -Spalte 4, Zeile 49 Spalte 36, Zeile 7 - Zeile 39	5,6,9
X	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19. März 1998 (1998-03-19) Seite 3, Zeile 22 -Seite 5, Zeile 25 Seite 10, Zeile 11 -Seite 11, Zeile 30	1,2, 7-10,15, 17,18
Y	US 5 280 527 A (FAST NORMAN ET AL) 18. Januar 1994 (1994-01-18) Zusammenfassung Spalte 5, Zeile 34 - Zeile 54	5,6,9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. November 2000	09/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Teutloff, H

Formblan PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/07124

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5870723 A	09-02-1999	US 5613012 A	18-03-1997
		US 5615277 A	25-03-1997
		AU 4329597 A	19-03-1998
		WO 9809227 A	05-03-1998
		US 6012039 A	04-01-2000
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		EP 0912959 A	06-05-1999
		JP 11511882 T	12-10-1999
		WO 9636934 A	21-11-1996
		US 5838812 A	17-11-1998
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
		EP 0931430 A	28-07-1999
US 5280527 A	18-01-1994	CA 2105404 A	03-03-1995

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT) T15

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
K 51 513/7 so		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP00/07124	25/07/2000	30/07/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G07C9/00		
Anmelder GIESECKE & DEVRIENT GMBH et al		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 4 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
06/02/2001	27.08.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter van der Haegen, D Tel. Nr. +49 89 2399 2683

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP00/07124

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

2-4	ursprüngliche Fassung			
1	eingegangen am	26/07/2001	mit Schreiben vom	26/07/2001

Patentansprüche, Nr.:

1-18	eingegangen am	26/07/2001	mit Schreiben vom	26/07/2001

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:

☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	4, 7, 12-14, 16-17
	Nein:	Ansprüche	1-3, 5-6, 8-11, 15, 18
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	12-13
	Nein:	Ansprüche	1-11, 14-18
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-18
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Es wird auf die folgenden Dokumente verwiesen:

   D1: WO 98 11750 A (SUBBIAH SUBRAMANIAN) 19. März 1998,
   D2: US-A-5 870 723 (HOFFMAN NED ET AL) 9. Februar 1999 und
   D3: US-A-5 280 527 (FAST NORMAN ET AL) 18. Januar 1994.

2. **Artikel 33(2) PCT**

2.1 Dokument D1, das als nächstliegender Stand der Technik angesehen wird, offenbart ein Verfahren zur Sicherung einer biometrischen Authentisierung einer Telefonverbindung gegen Replay-Angriffe (vgl. Seite 1, Zeilen 18-20 und Seite 4, Zeilen 27-35), wobei :

- durch ein Program (vgl. Figur 6, Bezugszeichen 606) eines zentralen Authentisierungssystems (vgl. Figur 6, Bezugszeichen 106) ein Vergleich zwischen den in einem "MIN Challenge Key" Datenspeicher (vgl. Figur 1, Bezugszeichen 7) als "Challenge Key" (vgl. Figur 2, Bezugszeichen 202) gespeicherten biometrischen Daten einer Person und durch ein "Fingerprint Capturing" Modul (vgl. Figur 1, Bezugszeichen 101) als "Token" erneut erfaßten biometrischen Daten der Person durchgeführt wird (vgl. Seite 10, Zeilen 3-8),
- eine Authentisierung der Telefonverbindung erfolgt, wenn eine Übereinstimmung innerhalb einer vorgegebenen Toleranz liegt (vgl. Seite 11, Zeilen 26-28 und Seite 14, Zeilen 14-23, 35-36; Figur 3B, Schritt 313) und
- die Telefonverbindung gesperrt wird, wenn durch den Vergleich eine identische Übereinstimmung des "Token" mit dem "Challenge Key" festgestellt wird (vgl. Seite 10, Zeilen 11-30 und Seite 14, Zeilen 24-34; Figur 3B, Schritt 320).

Das Verfahren gemäß Anspruch 1 unterscheidet sich nicht vom Verfahren gemäß D1. Der Gegenstand des unabhängigen Anspruchs 1 ist somit nicht neu.

2.2 D1 offenbart ferner eine Vorrichtung zur biometrischen Authentisierung, umfassend :

- einen "MIN Challenge Key" Datenspeicher (vgl. Figur 1, Bezugszeichen 107) mit "Challenge Keys" (vgl. Figur 2, Bezugszeichen 202) als biometrischen Referenzdaten und
- ein Program (vgl. Figur 6, Bezugszeichen 606) zur Durchführung des unter Punkt 2.1 beschriebenen Verfahren.

Die Vorrichtung gemäß Anspruch 8 unterscheidet sich nicht von der Vorrichtung gemäß D1. Der Gegenstand des unabhängigen Anspruchs 8 ist somit nicht neu.

2.3 Die von den abhängigen Ansprüchen 2-3, 5-6, 9-11, 15 und 18 eingeführten Merkmale sind aus D1 bekannt und fügen somit den Ansprüchen 1 und 8 nichts hinzu, was die Gegenstände der Ansprüche 1, 8 neu machen würde :

- für Ansprüche 2 und 10, siehe D1, z.B. Seite 14, Zeilen 24-34, "(...)identisch(...)",
- für Ansprüche 3 und 11, siehe D1, z.B. Seite 14, Zeilen 24-34,
- für Ansprüche 5, 6 und 9, siehe D1, z.B. Figur 1, Bezugszeichen 106 und 107,
- für Anspruch 15, siehe D1, z.B. Seite 14, Zeilen 24-34 und Figur 3B, Schritt 315, "Block" und
- für Anspruch 18, siehe D1, z.B. Figur 1, Bezugszeichen 101.

3. Artikel 33(3) PCT

3.1 Die von den abhängigen Ansprüchen 4, 7, 14 und 16-17 eingeführten Merkmale scheinen, im Licht des vorhandenen Standes der Technik, übliche konstruktive Maßnahmen zu betreffen und/oder im Rahmen dessen zu liegen, was ein Fachmann aufgrund der ihm geläufigen Überlegungen zu tun pflegt. Deshalb fügen die genannten Ansprüche den Ansprüchen 1, 8 keine Merkmale hinzu, die

eine erfinderische Tätigkeit begründen würden :

- Ansprüche 4 und 14 : das Festlegen des Schwellwerts bei 99% ist eine übliche konstruktive Maßnahme zur Lösung der den Ansprüchen 4 und 14 zugrundeliegenden Aufgabe,
- Ansprüche 7 und 17 : das Verschlüsseln von erfaßten biometrischen Daten ist aus Dokument D3 bekannt (vgl. Spalte 5, Zeilen 15-19). Für den Fachmann wäre deswegen das Bilden eines Hashwerts aus den erfaßten biometrischen Daten, zumal die damit erreichte Vorteile ohne weiteres im voraus zu übersehen sind, eine naheliegende, im Rahmen normalen fachlichen Handelns liegende Vorgehensweise zur Lösung der den Ansprüchen 7 und 17 zugrundeliegenden Aufgabe, und
- Anspruch 16 : das Ausgeben einer Fehlermeldung bei Verweigerung der Authentisierung ist aus Dokument D2 bekannt (vgl. Figur 16, "Error message"; Spalte 5, Zeilen 1-4). Für den Fachmann wäre die Aufnahme dieses Merkmal in die in D1 beschriebene Vorrichtung eine naheliegende Vorgehensweise zur Lösung der dem Anspruch 16 zugrundeliegenden Aufgabe.

3.2 Die Gegenstände der abhängigen Ansprüche 12 und 13 dürften die Kriterien der Neuheit und erfinderischen Tätigkeit gemäß Artikel 33(2) und (3) PCT erfüllen.

4. Artikel 33(4) PCT

Gewerbliche Anwendbarkeit der Ansprüche 1-18 ist offensichtlich gegeben.

Verfahren und Vorrichtung zur biometrischen Authentisierung

Die Erfindung betrifft ein Verfahren sowie eine Vorrichtung zur biometrischen Authentisierung, insbesondere zur Sicherung der biometrischen Authentisierung gegen Replay-Angriffe.

Ein Authentisierungsverfahren findet Anwendung, wenn eine Person Zugang zu gesicherten Einrichtungen begehrt. Beispielsweise erfolgt eine Authentisierung regelmäßig mittels eines PIN-Vergleichs, wenn ein Kartenbenutzer eine Chipkarte - beispielsweise eine Kreditkarte - in einen Bankautomaten (Terminal) einführt oder wenn eine Person zu zugangsgesicherten Räumlichkeiten Eintritt begehrt. Dazu wird eine gespeicherte PIN mit der vom Kartenbenutzer bzw. von der Eintritt begehrenden Person angegebenen PIN auf Identität überprüft.

Im Falle eines biometrischen Authentisierungsverfahrens wird anstatt einer PIN ein biometrisches Merkmal der Person als Identifikationsmerkmal benutzt. Das biometrische Merkmal kann beispielsweise ein Fingerabdruck sein, soll im Sinne der vorliegenden Erfindung aber auch eine persönliche Unterschrift umfassen. Nachteilhaft bei solchen Authentisierungsverfahren ist, daß ein Angriff auf die Authentisierung möglich ist, wenn die biometrischen Daten, die als Referenzdaten abgespeichert wurden oder die zu einer Authentisierung geführt haben, von nicht autorisierten Dritten abgefangen werden, um sie später erneut für eine unberechtigte Authentisierung zu verwenden. Diese Art des Angriffs wird als Replay-Angriff bezeichnet. Aus WO 98/11750 A2 ist ein Verfahren zur Verhinderung von Replay-Angriffen bekannt, bei dem die verschlüsselten, digitalen Daten von Fingerabdrücken gespeichert werden. Werden zu einem späteren Zeitpunkt identische Daten eingegeben, wird die Authentisierung verweigert.

Aufgabe der vorliegenden Erfindung ist es daher, ein Verfahren sowie eine Vorrichtung zur biometrischen Authentisierung gegen Replay-Angriffe sicherer zu gestalten.

Patentansprüche

1. Verfahren zur Sicherung einer biometrischen Authentisierung gegen Replay-Angriffe, wobei ein Vergleich zwischen als Referenzdaten gespeicherten biometrischen Daten einer Person und erneut erfaßten biometrischen Daten der Person auf Übereinstimmung durchgeführt wird und eine Authentisierung erfolgt, wenn die Übereinstimmung gleich oder größer einem vorgegebenen ersten Schwellwert ist, **dadurch gekennzeichnet,** daß die Authentisierung verweigert wird, wenn durch den Vergleich eine Übereinstimmung der erneut erfaßten biometrischen Daten mit den gespeicherten Referenzdaten festgestellt wird, die gleich oder größer einem vorgegebenen zweiten Schwellwert ist.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß der zweite Schwellwert bei 100%iger Übereinstimmung festgelegt wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet,** daß die bei verschiedenen Authentisierungsvorgängen erfaßten biometrischen Daten als Datensätze gesammelt und gespeichert werden und die Authentisierung verweigert wird, wenn die erneut erfaßten biometrischen Daten eines aktuellen Authentisierungsvorgangs im Vergleich zu einem der gespeicherten Datensätze eine über dem vorgegebenen zweiten Schwellwert liegende Übereinstimmung aufweisen.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** daß der zweite Schwellwert bei mindestens 99%iger Datenübereinstimmung festgelegt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß die Referenzdaten und gegebenenfalls die Datensätze auf einem Datenträger, insbesondere einer Chipkarte, gespeichert werden.

6. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß die Referenzdaten und gegebenenfalls die Datensätze in einer Authentisierungsvorrichtung, insbesondere einem Chipkartenterminal, gespeichert werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet,** daß aus den erneut erfaßten biometrischen Daten ein Hashwert gebildet wird und daß die gespeicherten Referenzdaten ein Hashwert sind.

8. Vorrichtung zur biometrischen Authtisierung, umfassend einen ersten Speicherbereich mit biometrischen Daten als Referenzdaten und eine Vergleichsschaltung, die eine Meldung erzeugt, welche die Authentisierung zuläßt, wenn ein Vergleich der Referenzdaten mit neu erfaßten biometrischen Daten einer Person eine Übereinstimmung ergibt, die gleich oder größer einem gegebenen ersten Schwellwert ist, **dadurch gekennzeichnet,** daß die Vergleichsschaltung eine Meldung erzeugt, welche die Authentisierung verweigert, wenn ein Vergleich der Refernzdaten mit neu erfaßten biometrischen Daten einer Person eine Übereinstimmung ergibt, die gleich oder größer einem gegebenen zweiten Schwellwert ist.

9. Vorrichtung nach Anspruch 8, **dadurch gekennzeichnet,** daß die Vorrichtung ein Datenträger, insbesondere eine Chipkarte, ist.

10. Vorrichtung nach Anspruch 8 oder 9, **dadurch gekennzeichnet,** daß der zweite Schwellwert auf 100% eingestellt ist.

11. Vorrichtung nach einem der Ansprüche 8 bis 10, **gekennzeichnet durch** weitere Speicherbereiche , in denen mehrere Datensätze von erneut erfaßten biometrischen Daten gespeichert sind.

12. Vorrichtung nach Anspruch 11, **dadurch gekennzeichnet**, daß die weiteren Speicherbereiche einen Stapelspeicher bilden.

13. Vorrichtung nach Anspruch 11, **dadurch gekennzeichnet**, daß die weiteren Speicherbereiche ein Schieberegister bilden.

14. Vorrichtung nach einem der Ansprüche 8 bis 13, **dadurch gekennzeichnet**, daß der zweite Schwellwert auf einen Wert ≥ 99% eingestellt ist.

15. Vorrichtung nach einem der Ansprüche 8 bis 14, **dadurch gekennzeichnet**, daß sich die Vorrichtung bei Vorliegen der Meldung der Verweigerung der Authentisierung automatisch sperrt.

16. Vorrichtung nach einem der Ansprüche 8 bis 15, **dadurch gekennzeichnet**, daß die Vorrichtung bei Vorliegen der Meldung der Verweigerung der Authentisierung eine Fehlermeldung ausgibt.

17. Vorrichtung nach einem der Ansprüche 8 bis 16, **dadurch gekennzeichnet**, daß im ersten Speicherbereich als Referenzdaten ein aus biometrischen Daten abgeleiteter Hashwert gespeichert ist und daß die Vergleichsschaltung aus den neu erfaßten biometrischen Daten einen Hashwert für den Vergleich mit den gespeicherten Referenzdaten bildet.

18. Vorrichtung nach einem der Ansprüche 8 bis 17, **dadurch gekennezeichnet**, daß die Vorrichtung eine Einrichtung zum Erfassen biometrischer Daten einer Person aufweist.

Translation
10/030164
5000

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference K 51 513/7ch	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP00/07124	International filing date (*day/month/year*) 25 July 2000 (25.07.00)	Priority date (*day/month/year*) 30 July 1999 (30.07.99)
International Patent Classification (IPC) or national classification and IPC G07C 9/00		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
06 February 2001 (06.02.01)	27 August 2001 (27.08.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELI[redacted]ARY EXAMINATION REPORT

International application No.
[redacted] PCT/EP00/07124

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☒ the international application as originally filed.

☒ the description, pages 2-4, as originally filed,
pages _____, filed with the demand,
pages 1, filed with the letter of 26 July 2001 (26.07.2001),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-18, filed with the letter of 26 July 2001 (26.07.2001),
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
EP 00/07124

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	4, 7, 12-14, 16-17	YES
	Claims	1-3, 5-6, 8-11, 15, 18	NO
Inventive step (IS)	Claims	12-13	YES
	Claims	1-11, 14-18	NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: WO-A-98/11750 (SUBBIAH SUBRAMANIAN) 19 March 1998
D2: US-A-5 870 723 (HOFFMAN NED ET AL) 9 February 1999
D3: US-A-5 280 527 (FAST NORMAN ET AL) 18 January 1994

2. **PCT Article 33(2)**

2.1. Document D1, which is the closest prior art, discloses a method for securing a biometric authentication of a telephone connection against replay attacks (cf. page 1, lines 18-20 and page 4, lines 27-35):

- a program (cf. Figure 6, reference sign 606) of a central authentication system (cf. Figure 6, reference sign 106) performing a comparison between a person's biometric data that has been stored as a "challenge key" (cf. Figure 2, reference sign 202) in an "MIN challenge key" data memory (cf. Figure 1, reference sign 7) and the person's biometric data that has been re-registered as a "token" (cf. page 10, lines 3-8) by a "fingerprint capturing" module (cf. Figure 1, reference sign 101),
- an authentication of the telephone connection occurring when there is agreement within a predetermined tolerance (cf. page 11, lines 26-28 and page 14, lines 14-23, 35-36; Figure 3B, step 313)

and

- the telephone connection being blocked if the comparison determines that there is identical agreement between the "token" and the "challenge key" (cf. page 10, lines 11-30 and page 14, lines 24-34; Figure 3B, step 320).

The method according to Claim 1 does not differ from the method according to D1. The subject matter of independent Claim 1 is thus not novel.

2.2. D1 also discloses a device for biometric authentication encompassing:

- an "MIN challenge key" data memory (cf. Figure 1, reference sign 107) with "challenge keys" (cf. Figure 2, reference sign 202) as biometric reference data and
- a program (cf. Figure 6, reference sign 606) for carrying out the method described in point 2.1.

The device according to Claim 8 does not differ from the device according to D1. The subject matter of independent Claim 8 is thus not novel.

2.3. The features introduced by dependent Claims 2-3, 5-6, 9-11, 15 and 18 are known from D1 and add nothing that would render the subject matter of Claims 1 and 8 novel:

- Claims 2 and 10: see D1, e.g. page 14, lines 24-34, "...identical...";
- Claims 3 and 11: see D1, e.g. page 14, lines 24-34;
- Claims 5, 6 and 9: see D1, e.g. Figure 1, reference signs 106 and 107;
- Claim 15: see D1, e.g. lines 24-34 and Figure 3B, step 315, "block"; and
- Claim 18: see D1, e.g. Figure 1, reference sign 101.

3. **PCT Article 33(3)**

3.1. In light of the available prior art, the features introduced by dependent Claims 4, 7, 14 and 16-17 appear to relate to routine design measures and/or would be straightforward for a person skilled in the art. Therefore the above-mentioned claims do not add any features to Claims 1 and 8 that would constitute an

inventive step:

- Claims 4 and 14: setting the threshold value at 99% is a routine design measure to solve the problem addressed by Claims 4 and 14;
- Claims 7 and 17: encrypting the registered biometric data is known from document D3 (cf. column 5, lines 15-19). Generating a hash value from the registered biometric data would be straightforward for a person skilled in the art, especially since the resulting advantages are readily foreseeable in solving the problem addressed by Claims 7 and 17; and
- Claim 16: displaying an error message when authentication is denied is known from document D2 (cf. Figure 16, "error message"; column 5, lines 1-4). Incorporating this feature into the device described in D1 would represent to a person skilled in the art an obvious approach in solving the problem addressed by Claim 16.

3.2. The subject matter of dependent Claims 12 and 13 appears to fulfill the criteria of PCT Article 33(2) and (3) with respect to novelty and inventive step.

4. **PCT Article 33(4)**

The industrial applicability of Claims 1-18 is clearly established.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 April 2001 (06.04.01)	
International application No. PCT/EP00/07124	**Applicant's or agent's file reference** K 51 513/7ch
International filing date (day/month/year) 25 July 2000 (25.07.00)	**Priority date** (day/month/year) 30 July 1999 (30.07.99)
Applicant MÖDL, Albert et al	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   06 February 2001 (06.02.01)

   [ ] in a notice effecting later election filed with the International Bureau on:

   _____

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Nestor Santesso
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT [redacted] DEM GEBIET DES PATENTWE[redacted]NS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts K 51 513/7ch	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/EP 00/ 07124	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 25/07/2000	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 30/07/1999
Anmelder GIESECKE & DEVRIENT GMBH		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. ---

   [ ] wie vom Anmelder vorgeschlagen [X] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
[redacted]/EP 00/07124

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 870 723 A (HOFFMAN NED ET AL) 9. Februar 1999 (1999-02-09)	1-3,8, 10,11, 15,16,18
Y	Spalte 2, Zeile 11 -Spalte 4, Zeile 49 Spalte 36, Zeile 7 - Zeile 39	5,6,9
X	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19. März 1998 (1998-03-19) Seite 3, Zeile 22 -Seite 5, Zeile 25 Seite 10, Zeile 11 -Seite 11, Zeile 30	1,2, 7-10,15, 17,18
Y	US 5 280 527 A (FAST NORMAN ET AL) 18. Januar 1994 (1994-01-18) Zusammenfassung Spalte 5, Zeile 34 - Zeile 54	5,6,9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. November 2000	09/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Teutloff, H

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
[redacted]/EP 00/07124

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5870723 A	09-02-1999	US 5613012 A	18-03-1997
		US 5615277 A	25-03-1997
		AU 4329597 A	19-03-1998
		WO 9809227 A	05-03-1998
		US 6012039 A	04-01-2000
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		EP 0912959 A	06-05-1999
		JP 11511882 T	12-10-1999
		WO 9636934 A	21-11-1996
		US 5838812 A	17-11-1998
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
		EP 0931430 A	28-07-1999
US 5280527 A	18-01-1994	CA 2105404 A	03-03-1995